

Blockchain, Cryptocurrencies, and Security

For John Jay FCM 740 by Mike Fernez

Cutting through some confusion...

- Digital currency-an intangible form of money issued by developers for use within a virtual community
 - e.g. Ven, Amazon Coin, Nintendo points, Warcraft Gold
- Cryptocurrency-a digital currency utilizing cryptography to secure and verify transactions
 - e.g. Bitcoin, Ethereum, Monero
- Blockchain-an open P2P distributed database system that records blocks of data in a way which is verifiable and cryptographically secure
 - e.g. not only cryptocurrencies but general purpose data systems such as Hyperledger which powers medical databases, anti-fraud software, i-voting and e-government systems

<https://en.wikipedia.org/wiki/Blockchain>

<https://www.hyperledger.org/about>

The Mysterious Birth of Blockchain

- Prior to Bitcoin in the 90s, there were some attempts to describe and implement digital cash by researchers who communicated through the cypherpunk mailing list
 - incl. Ecash (David Chaum), hashcash (Adam Back, Hal Finney), bit gold (Nick Szabo) powered by proof-of-work algorithms
 - The first citation of the Bitcoin paper is a link to a text document on Wei Dai's research website describing "b-money," a hypothetical money that could exist in a community without government and the protocols which could realize it.
 - Inspired by Tim May's "Cyphernomicon" and "Crypto-Anarchist Manifesto"
- In 2008, a white paper from an author by the name "Satoshi Nakamoto" was posted to a cryptography mailing list
 - Though there have been many claims, no one knows who Nakamoto is
 - The first real-world Bitcoin transaction was made by Laszlo Hanyecz in Florida: 10,000 BTC for two pizzas from Papa John's (~\$80 mil today)

https://en.wikipedia.org/wiki/History_of_bitcoin

https://www.wired.com/2011/11/mf_bitcoin/

<https://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html>

The Mysterious Birth of Blockchain

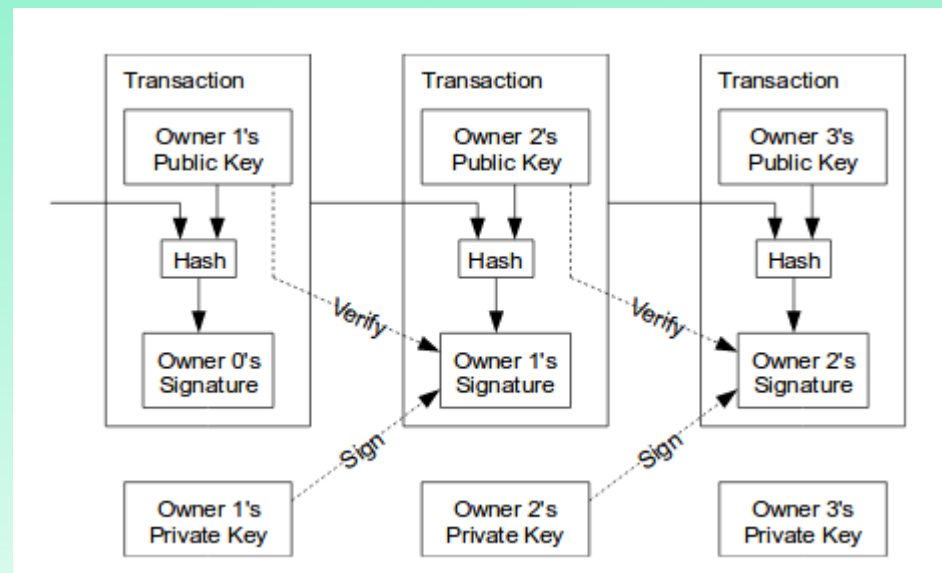
- This paper proposed two foundational ideas. Bitcoin, the cryptocurrency, and the blockchain it's engine
 - This paper came shortly after the 2008 financial crisis when trust in financial institutions was at an all time low
 - The Genesis block has the text: “The Times 03/Jan/2009 Chancellor on brink of second bailout for banks.”

https://en.bitcoin.it/wiki/Genesis_block
<http://www.thetimes03jan2009.com/>



The Nuts and Bolts of the Bitcoin Blockchain: Transaction Chain

- Nakamoto defines an electronic coin as “a chain of digital signatures.”
- This ensures the transaction is secure, but provides no method of validation



The Nuts and Bolts of the Bitcoin Blockchain: Timestamp Network

- The solution is to *announce* transactions to the entire network, order them, and then publish them permanently
- The process of sorting and validating blocks is handled by *miners*

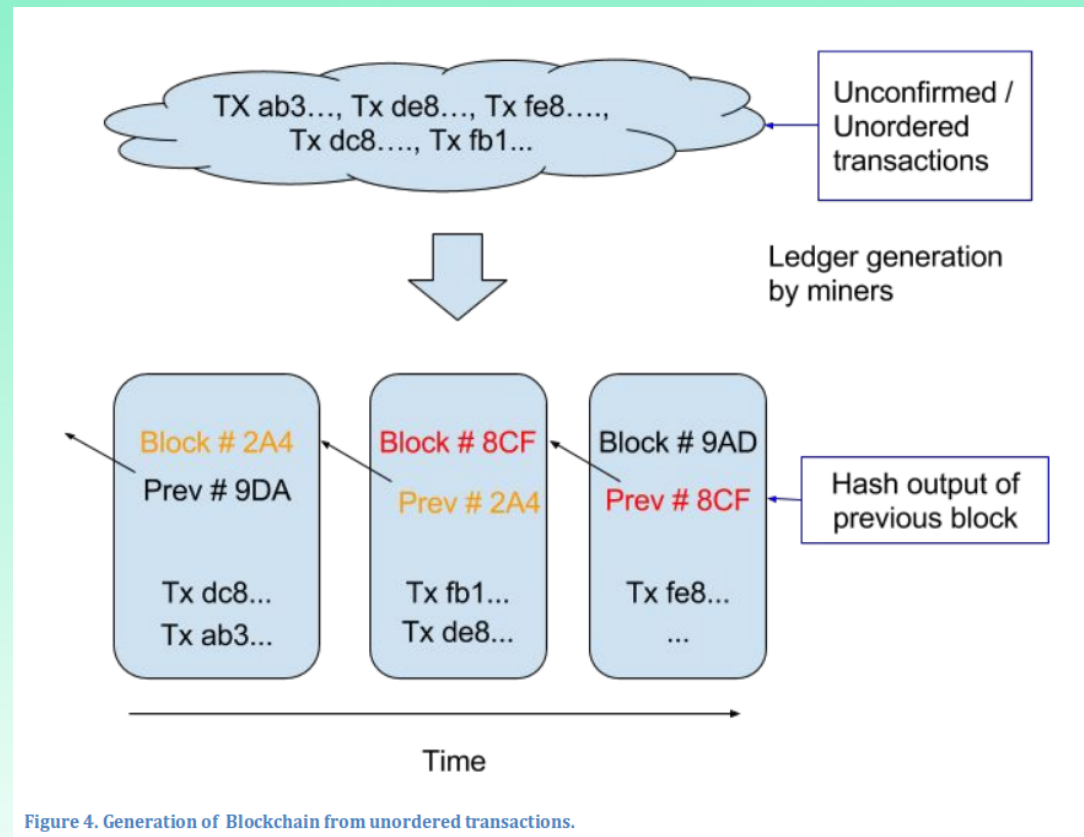
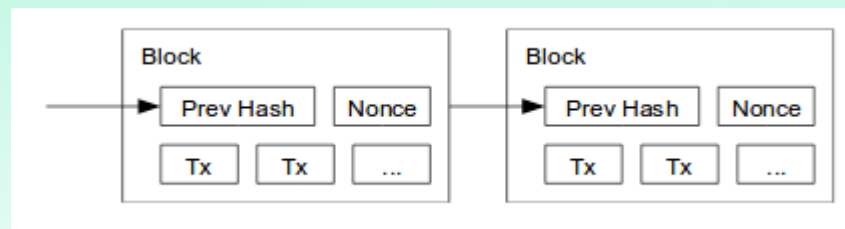


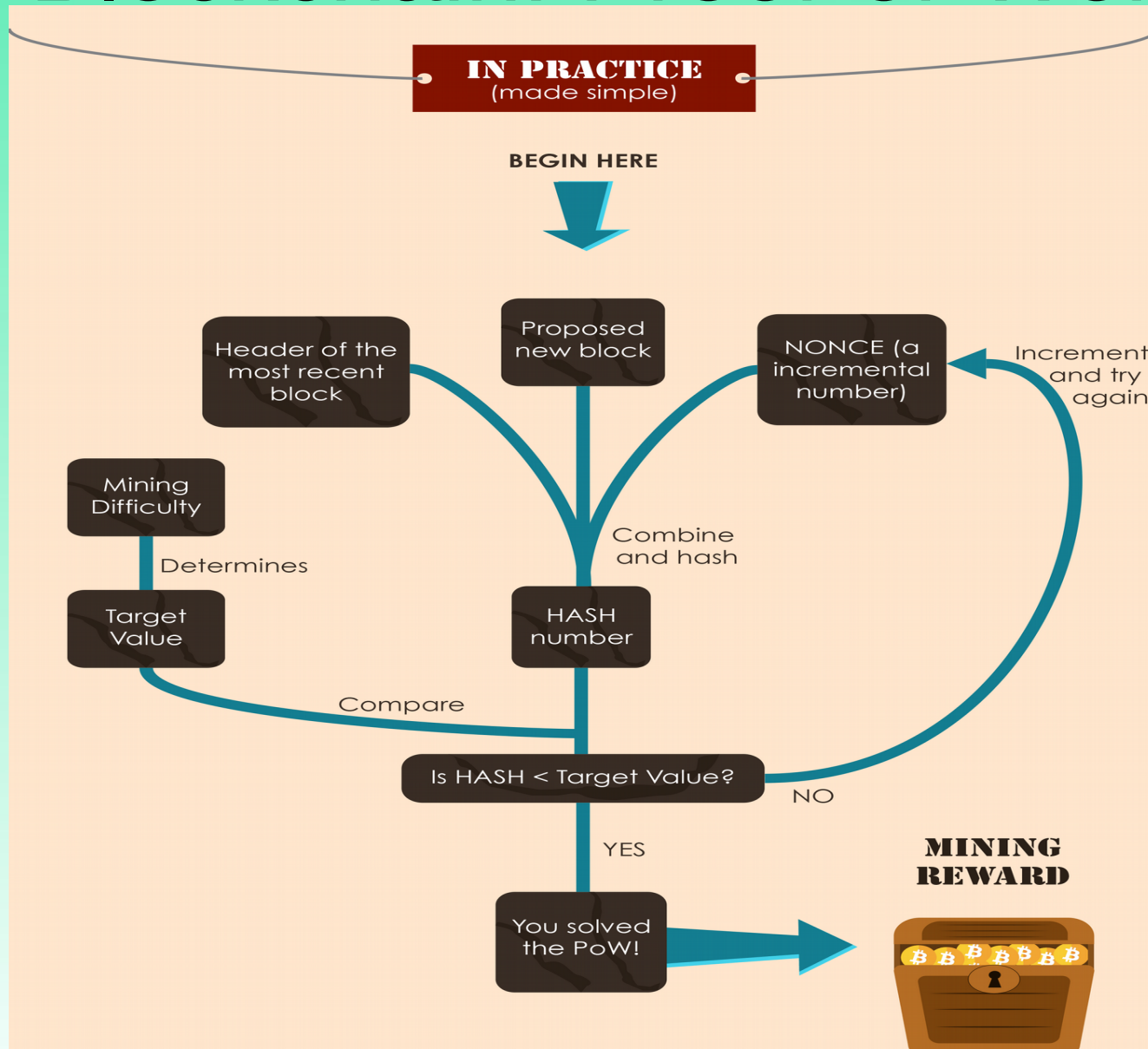
Figure 4. Generation of Blockchain from unordered transactions.

The Nuts and Bolts of the Bitcoin Blockchain: Proof-of-Work

- Proofs-of-work are the mechanism that govern how blocks are added and how miners get rewarded
 - A proof is achieved by miners looking for a number (n) that, with the hash of the block (b), yields a hash with a certain number of zero-bits (x)
 - Informally: when $H(\text{proposed block} + \text{newest block} + n) = x$
 - Finding the number is a hard problem, but verifying is just one hash
 - Bitcoin goes to the first CPU to solve it
- A dishonest node trying to change the record cannot do so without re-doing the work of the block and every block added after that



The Nuts and Bolts of the Bitcoin Blockchain: Proof-of-Work



The Nuts and Bolts of the Bitcoin Blockchain: Network Integrity

- As long as the network is distributed enough, any single attack on the network won't affect the availability of the blockchain
- In a formal proof, Nakamoto considers an attacker trying to broadcast a competing chain, allowing him to spend again
 - The probability of the attacker catching up decreases exponentially the longer the chain

p = probability an honest node finds the next block
 q = probability the attacker finds the next block
 q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \leq q \\ (q/p)^z & \text{if } p > q \end{cases} \quad \lambda = z \frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \begin{cases} (q/p)^{(z-k)} & \text{if } k \leq z \\ 1 & \text{if } k > z \end{cases}$$

All in all...

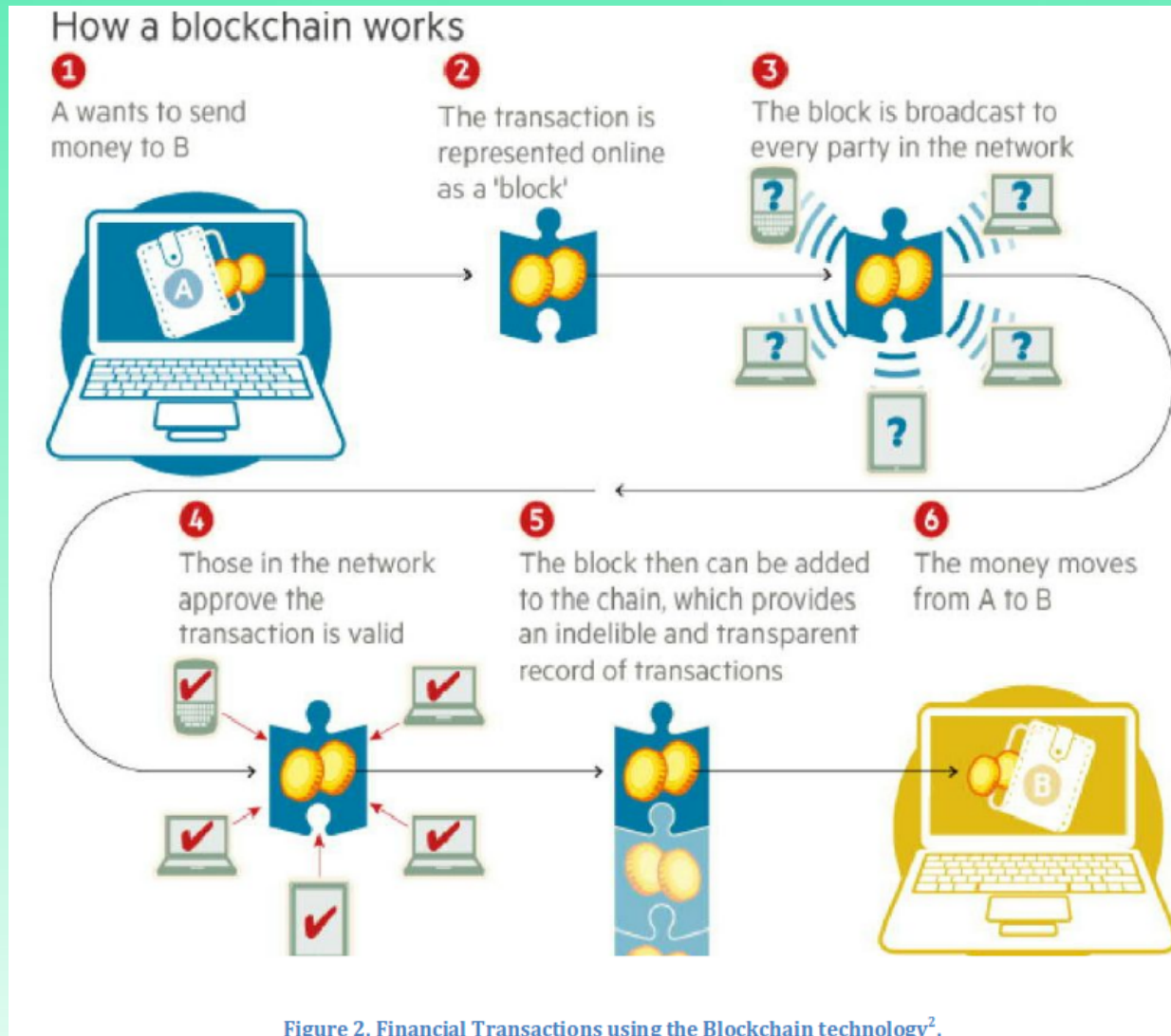


Figure 2. Financial Transactions using the Blockchain technology².

² <http://www.ft.com/intl/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html#axzz3qe4rV5dH>

All in all...

- The blockchain, provides Bitcoin transactions with layers of security:
 - Relative Anonymity (wallets are public keys)
 - Creates an immutable record of transactions
 - Network is distributed enough to resist attacks
- The Bitcoin protocol also encourages fair play by design:
 - The cost of CPU resources to defraud the ledger far outweighs the benefit one would gain from mining

A Brief Look At Cryptocurrencies

- “a general purpose blockchain”
 - **Ethereum** is a distributed virtual machine platform, designed to be programmable so it can execute smart contracts
 - “Ether” is the system’s currency
 - Currently hosts 1241 blockchain-based projects (including organizations like bitnation and games like cryptokitties)



<https://www.youtube.com/watch?v=WSN5BaCzsbo>
<https://www.stateofthedapps.com>

A Brief Look At Cryptocurrencies

- **Monero** (originally CryptoNote)

- A cryptocurrency designed for secure and anonymous transactions
- Utilizes a process called a “one-time ring signature” to obscure transactions.
- From the white paper review on Monero’s site:

We can imagine the CN protocol as a post-office-box system. Each user has a set of public keys and private keys, just like in the BTC protocol. Rather than sending CryptoNote directly to each others public keys, users execute a Diffie-Hellman exchange and create ring signatures to make a new one-time post-office-box at which the CNs are stored. And when we send our CN,we include our key image, which is just the hash of the private destination key that gave us the right to send those CN in the first place. If that key image has not yet been used, then that one-time ring signature has not yet been spent.

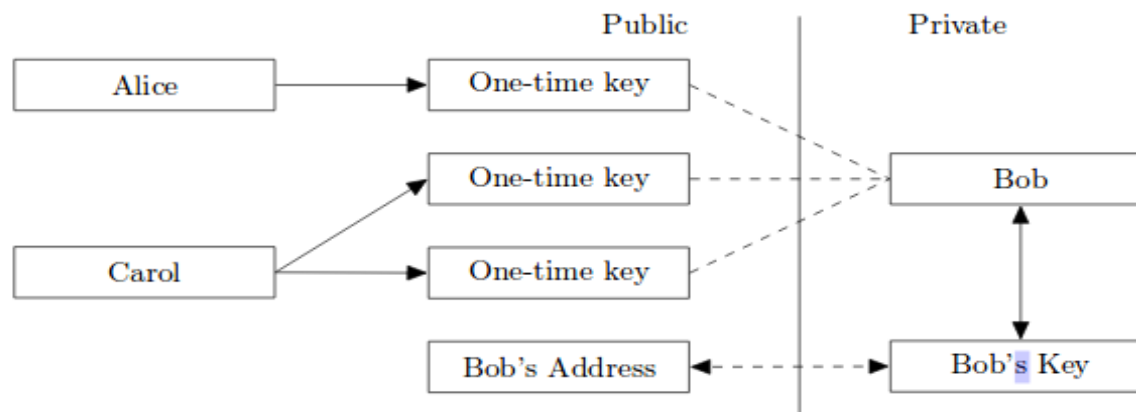


Fig. 3. CryptoNote keys/transactions model.

A Brief Look At Cryptocurrencies

- A million more...



<https://www.irta.com/wp-content/uploads/2016/02/cryptocurrency-01.jpg>

<https://i2.cdn.turner.com/cnnnext/dam/assets/140223132422-irpt-dogecoin-tech-4-horizontal-large-gallery.png>

<https://coinmarketcap.com/currencies/zcash/>

<http://static3.businessinsider.com/image/5a71a5e9ec1ade273f1f5aed-400/tethericon.png>

Use and Abuse Worldwide

- Cryptojacking
 - Spread wildly in the last year, esp. due to spread of browser crypto-mining extensions like Coinhive
 - Typically causes sharp rise in CPU use on a web browser or web site
 - This site can also help detect cryptojacking: <https://cryptojackingtest.com/>
 - DPRK notorious for this lately, attacking SK exchanges for Monero mining
- Ransomware
 - List of attacks grows longer and longer: CryptoLocker
 - US and UK have attributed WannaCry to DPRK
 - Atlanta became victim to a ransomware attack recently, locking up court and police files, causing internet outages, overall costing the city millions so far
- Venezuelan Crisis
 - With the Bolivar at a value lower than WOW gold, the Maduro government is putting its faith in issuing Petro, a cryptocurrency supposedly backed by oil

<https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-alternative-monero-cryptojacking-north-korea-alienvault-labs-a8149371.html>
<https://www.wired.com/story/cryptojacking-has-gotten-out-of-control/>

<https://www.npr.org/2018/03/30/598386485/atlanta-paralyzed-for-more-than-a-week-by-cyber-attack>
<https://www.cnn.com/2018/03/22/us/atlanta-ransomware-attack/index.html>
<https://www.npr.org/sections/thetwo-way/2017/12/19/571854614/u-s-says-north-korea-directly-responsible-for-wannacry-ransomware-attack>

<https://www.coindesk.com/petro-debut-learned-venezuelas-cryptocurrency-today/>
http://www.gameusd.com/game/product/index?server_id=1

Blockchain Explorers and Forensics

- Cryptocurrency Blockchains
 - Bitcoin- <https://blockchain.info/>
 - Ethereum- <https://etherscan.io/>
 - Zcash- <https://zcash.blockexplorer.com/>
 - Monero- <https://monerohash.com/explorer/>
- Proprietary and other investigation tools
 - <https://www.chainalysis.com/>
 - <https://crystalblockchain.com/>


Blockchain Explorers and Forensics

- Transaction example

WikiLeaks Addresses are identifiers which you use to send bitcoins to another person.

Summary		Transactions	
Address	1HB5XMLmzFVj8ALj6mFBsifRoD4miY36v	No. Transactions	26465
Hash 160	b169f2b0b866db05900b93a5d76345f18d3afb24	Total Received	4,042.49702363 BTC
Tools	Related Tags - Unspent Outputs	Final Balance	0 BTC

[Request Payment](#) [Donation Button](#)



Transactions (Oldest First) Filter ▾

dfa5a5160fd1014357daa9bdc7de467223e9b1893cef4ec9151eea351e1def08		2018-04-13 14:44:02
WikiLeaks ↗	→	33wvNiUkXJAJ85e4yXJxJVWtsKqWDsDFK4
		0.00009326 BTC
		-0.00011563 BTC

Transaction View information about a bitcoin transaction

dfa5a5160fd1014357daa9bdc7de467223e9b1893cef4ec9151eea351e1def08

1HB5XMLmzFVj... (WikiLeaks [↗](#))



33wvNiUkXJAJ85e4yXJxJVWtsKqWDsDFK4

0.00009326 BTC

0.00009326 BTC

Summary	
Size	222 (bytes)
Weight	888
Received Time	2018-04-13 14:44:02
Lock Time	Block: 518032
Included In Blocks	518033 (2018-04-13 14:50:15 + 6 minutes)
Confirmations	529 Confirmations
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	0.00011563 BTC
Total Output	0.00009326 BTC
Fees	0.00002237 BTC
Fee per byte	10.077 sat/B
Fee per weight unit	2.519 sat/WU
Estimated BTC Transacted	0.00009326 BTC
Scripts	Show scripts & coinbase

Blockchain Explorers and Forensics

- Most users get coins and cash out (to fiat) through cryptocurrency exchanges
- Popular exchanges:
 - <https://www.coinbase.com/>
 - <https://www.bitfinex.com/>
 - <https://www.gdax.com/>
 - <https://www.kraken.com/>
 - The rest can be found here:
<https://cryptocoincharts.info/markets/info>

Blockchain Generally

- The technology of blockchain itself allows for the easy creation and distribution of immutable records over the Internet
- Blockchains are useful in many areas:
 - IPFS and Storj are file-sharing services
 - Steemit is a blockchain-based social network with a currency as a reward for contributions
 - Namecoin is a blockchain implementation of DNS
 - Everledger and Block-Verify are anti-counterfeit systems
 - Musicians find smart contracts useful (Peer Tracks, Ujo)

Permissioned Blockchains

- Hyperledger, founded by the Linux Foundation is an umbrella project for general-purpose blockchains
 - Hyperledger Fabric by IBM has drawn a lot of attention for its “plug-and-play” approach to consensus, access control, and smart contracts
 - Specifically not a cryptocurrency. Instead of miners has “validating peers”
- In finance, companies are using blockchains like these for authentication, transactions, and contracts
 - Chain is an on-going project with NASDAQ, CITI, Visa, State Street
 - Medici, Blockstream smart-contracts for stocks

<http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf>
<https://www.hyperledger.org/projects/fabric>
https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
<https://chain.com/sequence/>

Blockchain in Healthcare

- Permissioned blockchains could allow doctors and patients access to records efficiently and privately
 - Serves a digital identity system
 - As in Bitcoin, records and a log of access to them are encrypted for privacy, but distributed to keep integrity.
 - One such start-up powered by Hyperledger Fabric and Ethereum is Medicalchain

Blockchain in Government

- Natural fit for a public record system
 - Estonia has taken the lead on this, with other nations experimenting
 - Also a generalized platform: <https://www.recordskeeper.co/>
- Secure e-Voting
 - Russia and many other countries have announced moving towards a blockchain-secured ballot box
 - <https://www.coindesk.com/moscows-blockchain-voting-platform-adds-service-for-high-rise-neighbors/>
 - Platforms and startups for general purpose:
 - <https://polys.me>
 - <https://followmyvote.com/>

E-Estonia

- The Estonian government has taken the lead on implementing many technologies as part of its E-Governance initiative, integrating the KSI blockchain (X-Road) around 2012
 - Used for securing medical data
 - System for public records, laws, and court systems
 - i-Voting and e-Residency linked to digital PKI
- Guardtime is the software company that developed the KSI blockchain and produces anti-tamper hardware, authentication, insurance security, and GDPR compliance tools on the same technology

<https://e-estonia.com/>

<https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/>

<https://guardtime.com/solutions>

www.courtal.com

But let's not lose our head...

- In spite of the many benefits blockchain can add to the integrity and security of data, there are some important disadvantages:
 - Proofs-of-work and maintaining networks cost tons of electricity, CPU power, and money
 - Network speed and data syncing is difficult
 - Blockchains need widespread distribution to be effective
 - Software complexity, forks, and flaws